(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104969232 B
(45)授权公告日 2018.01.12

(21)申请号 201380072915.7
(22)申请日 2013.03.13
(65)同一申请的已公布的文献号
申请公布号 CN 104969232 A
(43)申请公布日 2015.10.07
(85)PCT国际申请进入国家阶段日
2015.08.13
(86)PCT国际申请的申请数据
PCT/US2013/030742 2013.03.13
(87)PCT国际申请的公布数据
WO2014/142817 EN 2014.09.18
(73)专利权人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 A.范德文 P.V.拜祖
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张凌苗 陈岚
(51)Int.Cl.
G06F 21/56(2006.01)
(56)对比文件
US 8397306 B1,2013.03.12,
US 2008184373 A1,2008.07.31,
审查员 邢爽

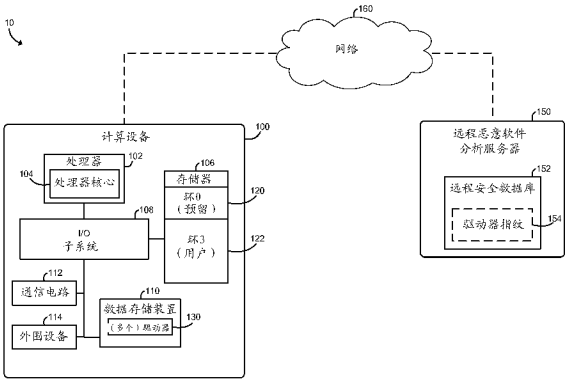
权利要求书4页 说明书15页 附图5页

(54)发明名称

管理设备驱动器跨环访问

(57)摘要

管理在计算设备上的设备驱动器的跨环存储器访问的技术包括:将与设备驱动器相关联的存储器页表配置为禁用设备驱动器的跨环存储器访问;截获设备驱动器的试图的跨环存储器访问;以及如果判定设备驱动器是恶意的则拒绝试图的跨环存储器访问。如果判定设备驱动器不是恶意的,则更新存储器页表以允许试图的跨环存储器访问。可以通过将设备驱动器和试图的跨环存储器访问与安全数据(例如存储于计算设备上的设备驱动器指纹和/或跨环存储器访问启发法)进行比较来分析设备驱动器,以判定设备驱动器是否是恶意的。



CN 104969232 B

1.一种用于管理在计算设备上的设备驱动器的跨环存储器访问的计算设备，所述计算设备包括：

安全模块，用于(i)将与所述设备驱动器相关联的存储器页表配置为禁用所述设备驱动器的跨环存储器访问，以及(ii)在配置相关联的存储器页表之后截获所述设备驱动器的试图的跨环存储器访问；以及

恶意软件分析模块，用于响应于截获所述试图的跨环存储器访问而分析所述设备驱动器和所述试图的跨环存储器访问，以判定所述设备驱动器是否是恶意的，

其中，所述安全模块还用于(i)响应于所述恶意软件分析模块判定所述设备驱动器是恶意的而拒绝所述试图的跨环存储器访问，或(i)响应于所述恶意软件分析模块判定所述设备驱动器不是恶意的，而更新与所述设备驱动器相关联的存储器页表，以允许所述试图的跨环存储器访问。

2.如权利要求1所述的计算设备，其中，所述恶意软件分析模块包括用于以下的恶意软件分析模块：

匹配所述设备驱动器与存储于本地安全数据库中的参考设备驱动器；以及

将所述参考设备驱动器的驱动器指纹与所述设备驱动器进行比较。

3.如权利要求2所述的计算设备，其中，所述恶意软件分析模块包括用于将所述驱动器指纹的地址与所述试图的跨环存储器访问所源自的所述设备驱动器的地址进行比较的恶意软件分析模块。

4.如权利要求3所述的计算设备，其中，所述恶意软件分析模块包括用于将预先定义的位屏蔽与和所述设备驱动器相关联的存储器页表进行比较的恶意软件分析模块。

5.如权利要求1所述的计算设备，其中，所述恶意软件分析模块包括用于以下的恶意软件分析模块：

判定所述设备驱动器是否与存储于本地安全数据库中的参考设备驱动器匹配；以及

响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考驱动器不匹配，而产生用于所述设备驱动器的驱动器指纹。

6.如权利要求1所述的计算设备，其中，所述恶意软件分析模块包括用于以下的恶意软件分析模块：

判定所述设备驱动器是否与存储于所述本地安全数据库中的参考设备驱动器匹配；以及

响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考设备驱动器不匹配，而更新与所述设备驱动器相关联的存储器页表以允许所述试图的跨环存储器访问。

7.如权利要求1所述的计算设备，其中，所述恶意软件分析模块包括用于以下的恶意软件分析模块：将所述试图的跨环存储器访问的目的地址与先前跨环存储器访问到所述目的地址的启发数据进行比较。

8.一种用于管理在计算设备上的设备驱动器的跨环存储器访问的方法，所述方法包括：

在所述计算设备上，将与所述设备驱动器相关联的存储器页表配置为禁用所述设备驱动器的跨环存储器访问；

在配置相关联的存储器页表之后，截获所述设备驱动器的试图的跨环存储器访问；

响应于截获所述试图的跨环存储器访问而分析所述设备驱动器和所述试图的跨环存储器访问，以判定所述设备驱动器是否是恶意的；

响应于判定所述设备驱动器是恶意的而拒绝所述试图的跨环存储器访问；以及

响应于判定所述设备驱动器不是恶意的，而更新与所述设备驱动器相关联的存储器页表，以允许所述试图的跨环存储器访问。

9.如权利要求8所述的方法，其中，分析所述设备驱动器包括：

匹配所述设备驱动器与存储于本地安全数据库中的参考设备驱动器；以及

将所述参考设备驱动器的驱动器指纹与所述设备驱动器进行比较。

10.如权利要求9所述的方法，其中，比较所述驱动器指纹包括：将所述驱动器指纹的地址与所述试图的跨环存储器访问所源自的所述设备驱动器的地址进行比较。

11.如权利要求9所述的方法，其中，比较所述驱动器指纹包括：将预先定义的位屏蔽与和所述设备驱动器相关联的存储器页表进行比较。

12.如权利要求10所述的方法，其中，分析所述设备驱动器包括：

判定所述设备驱动器是否与存储于本地安全数据库中的参考设备驱动器匹配；以及

响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考设备驱动器不匹配，而更新与所述设备驱动器相关联的存储器页表以允许所述试图的跨环存储器访问。

13.如权利要求10所述的方法，其中，分析所述试图的跨环存储器访问包括：将所述试图的跨环存储器访问的目的地址与先前跨环存储器访问到所述目的地址的启发数据进行比较。

14.一种用于管理在计算设备上的设备驱动器的跨环存储器访问的计算设备，所述计算设备包括：

用于在所述计算设备上将与所述设备驱动器相关联的存储器页表配置为禁用所述设备驱动器的跨环存储器访问的装置；

用于在配置相关联的存储器页表之后截获所述设备驱动器的试图的跨环存储器访问的装置；

用于响应于截获所述试图的跨环存储器访问而分析所述设备驱动器和所述试图的跨环存储器访问以判定所述设备驱动器是否是恶意的装置；

用于响应于判定所述设备驱动器是恶意的而拒绝所述试图的跨环存储器访问的装置；以及

用于响应于判定所述设备驱动器不是恶意的，而更新与所述设备驱动器相关联的存储器页表，以允许所述试图的跨环存储器访问的装置。

15.如权利要求14所述的计算设备，其中，用于分析所述设备驱动器的装置包括：

用于匹配所述设备驱动器与存储于本地安全数据库中的参考设备驱动器的装置；以及

用于将所述参考设备驱动器的驱动器指纹与所述设备驱动器进行比较的装置。

16.如权利要求15所述的计算设备，其中，用于比较所述驱动器指纹的装置包括：用于将所述驱动器指纹的地址与所述试图的跨环存储器访问所源自的所述设备驱动器的地址进行比较的装置。

17.如权利要求15所述的计算设备，其中，用于比较所述驱动器指纹的装置包括：用于将预先定义的位屏蔽与和所述设备驱动器相关联的存储器页表进行比较的装置。

18.如权利要求14所述的计算设备，其中，用于分析所述设备驱动器的装置包括：

用于判定所述设备驱动器是否与存储于本地安全数据库中的参考设备驱动器匹配的装置；以及

用于响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考驱动器不匹配，而产生用于所述设备驱动器的驱动器指纹的装置。

19.如权利要求14所述的计算设备，其中，用于分析所述设备驱动器的装置包括：

用于判定所述设备驱动器是否与存储于本地安全数据库中的参考设备驱动器匹配的装置；以及

用于响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考设备驱动器不匹配，而更新与所述设备驱动器相关联的存储器页表以允许所述试图的跨环存储器访问的装置。

20.如权利要求19所述的计算设备，其中，用于分析所述试图的跨环存储器访问的装置包括：用于将所述试图的跨环存储器访问的目的地址与先前跨环存储器访问到所述目的地址的启发数据进行比较的装置。

21.一种其上存储有指令的机器可读介质，所述指令当被执行时使得计算设备执行根据权利要求8-13中任一项所述的方法。

22.一种用于管理在计算设备上的设备驱动器的跨环存储器访问的装置，所述装置包括：

用于在所述计算设备上，将与所述设备驱动器相关联的存储器页表配置为禁用所述设备驱动器的跨环存储器访问的构件；

用于在配置相关联的存储器页表之后，截获所述设备驱动器的试图的跨环存储器访问的构件；

用于响应于截获所述试图的跨环存储器访问而分析所述设备驱动器和所述试图的跨环存储器访问，以判定所述设备驱动器是否是恶意的的构件；

用于响应于判定所述设备驱动器是恶意的而拒绝所述试图的跨环存储器访问的构件；以及

用于响应于判定所述设备驱动器不是恶意的，而更新与所述设备驱动器相关联的存储器页表，以允许所述试图的跨环存储器访问的构件。

23.如权利要求22所述的装置，其中，用于分析所述设备驱动器的构件包括：

用于匹配所述设备驱动器与存储于本地安全数据库中的参考设备驱动器的构件；以及

用于将所述参考设备驱动器的驱动器指纹与所述设备驱动器进行比较的构件。

24.如权利要求23所述的装置，其中，用于比较所述驱动器指纹的构件包括：用于将所述驱动器指纹的地址与所述试图的跨环存储器访问所源自的所述设备驱动器的地址进行比较的构件。

25.如权利要求23所述的装置，其中，用于比较所述驱动器指纹的构件包括：用于将预先定义的位屏蔽与和所述设备驱动器相关联的存储器页表进行比较的构件。

26.如权利要求24所述的装置，其中，用于分析所述设备驱动器的构件包括：

用于判定所述设备驱动器是否与存储于本地安全数据库中的参考设备驱动器匹配的构件；以及

用于响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考设备驱动器不匹配，而更新与所述设备驱动器相关联的存储器页表以允许所述试图的跨环存储器访问的构件。

27.如权利要求24所述的装置，其中，用于分析所述试图的跨环存储器访问的构件包括：用于将所述试图的跨环存储器访问的目的地址与先前跨环存储器访问到所述目的地址的启发数据进行比较的构件。

管理设备驱动器跨环访问

背景技术

[0001] 许多计算机架构实现某种形式的层级保护域或“环”。每个保护环具有相关联的权限模式(即,从高权限模式到低权限模式)。计算设备的操作系统例如通常在最高权限模式下执行。在软件领域,具有最高权限的保护环通常被称作“环0”或内核模式,较低权限环被分配有渐增的数字(如,环1、环2、环3等)。虽然特定的计算机架构或操作系统可以利用任意数量的保护环,但是一些计算机架构或操作系统利用仅具有几个保护环(如,仅有环0和环3)的减少的保护环方案。使用保护域或环允许对应的计算机系统对在每个保护环中执行的数据和应用提供保护,以免于在其它保护环内执行的那些的影响。例如,在一些计算机系统中,跨环访问(如,环0到环3访问)可能是受限的或者甚至是禁止的。

[0002] 设备驱动器是控制计算系统的特定设备的软件程序。设备驱动器充当计算系统的操作系统或操作系统所执行的应用与对应的硬件设备之间的接口。在许多计算系统中,设备驱动器连同操作系统在高权限保护环(例如环0)中执行。在另一方面,软件应用在较低权限环(例如环3)中执行。许多合法的设备驱动器在执行期间执行跨环访问(例如,环0到环3访问)。一些操作系统通过提供特定的应用接口程序(API)来促进跨环访问,所述应用接口程序必须由设备驱动使用来执行跨环访问而不引起扰乱。然而,许多设备驱动器可能不实现这样的API,或者另外被配置为以安全的方式执行跨环访问。这样,为了正常运转,计算机系统通常必须允许所有设备驱动器运行而没有任何跨环访问保护,或者全局地强制跨环访问保护,这使得传统设备驱动器停止正确运转。这样,对于提供在典型的使用各种设备设备的计算机系统中对存储器访问从较高保护环到较低保护环的跨环访问保护的能力受到限制。

附图说明

[0003] 本文所描述的概念是通过例子的方式而不是通过限制的方式在附图中进行图示的。为了图示的简洁和清晰,图中所图示的元件不必按照比例绘制。在认为合适之处,在图当中重复附图标记以指示对应或同类元件。

[0004] 图1是用于管理在计算设备上的(多个)设备驱动器跨环存储器访问的系统的至少一个实施例的简化框图;

[0005] 图2是图1的系统的计算设备的环境的至少一个实施例的简化框图;

[0006] 图3是图1和图2的计算设备的设备驱动器的可视化跨环存储器访问的简化图示;以及

[0007] 图4-6是用于管理在图1和图2的计算设备上的(多个)设备驱动器跨环存储器访问的方法的至少一个实施例的简化流程图。

具体实施方式

[0008] 虽然本公开的概念易于做出各种修改和替换形式,但其具体的实施例已经通过例子的方式在附图中示出并将在此详细描述。然而,应当理解的是,并不意图将本公开的概念

限制到所公开的具体形式，而是相反地，意图覆盖所有的与本公开和随附权利要求一致的修改、等价物和替代。

[0009] 说明书中提及“一个实施例”、“实施例”、“说明性实施例”等指示所描述的实施例可以包括特定特征、结构或特性，但是每个实施例可以或者可以不必包括所述特定特征、结构或特性。此外，这样的短语不必指代同一实施例。此外，当结合实施例描述特定特征、结构或特性时，应认为结合无论是否明确描述的其它实施例来实施这样的特征、结构或特性在本领域技术人员的认知范围内。

[0010] 在一些情况下，可以以硬件、固件、软件或其任意组合实现所公开的实施例。所公开的实施例还可以实现为瞬态或非瞬态机器可读(例如，计算机可读)存储介质所携带的或在其上存储的指令，该指令可以由一个或多个处理器读取和执行。机器可读存储介质可以体现为任意存储设备、机构、或用于存储或传输机器可读形式的信息的其它物理结构(例如，易失性或非易失性存储器、介质盘、或其它介质设备)。

[0011] 在图中，可以以具体布置和/或次序来示出一些结构或方法特征。然而，应当理解的是，可以不要求这样的具体布置和/或次序。而是在一些实施例中，这样的特征可以以不同于说明性的图中所示的方式和/或次序布置。另外，在特定图中包括结构或方法特征并不意味着暗示这样的特征在所有实施例中都需要，并且在一些实施例中，可以不包括这样的特征或者这样的特征可以与其它特征组合。

[0012] 现在参考图1，在说明性实施例中，用于管理跨环存储器访问的系统10包括计算设备100、远程恶意软件分析服务器150以及网络160，在网络160上计算设备100和远程恶意软件分析服务器150进行通信。计算设备100被配置为监控和管理由在计算设备100上执行的设备驱动器所执行的跨环存储器访问(例如，高权限到低权限存储器访问)。为此，如以下更详细讨论的，与每个设备驱动器相关联的存储器页表被配置为通过对应的设备驱动器禁用跨环存储器访问。也就是说，每个设备驱动器不能访问属于不同于该设备驱动器所属的保护环(例如，保护环0)的保护环(例如，保护环3)的存储器单元，而不引起异常或错误。任何跨环存储器访问被拦截或截获(trap)，并且进行调用的设备驱动器，和跨环存储器访问本身被分析以判定设备驱动器是否是恶意的。如果是，则拒绝试图的跨环存储器访问并可以中断设备驱动器。然而，如果设备驱动器被判定不是恶意的，则与进行调用的设备驱动器相关联的存储器页表被更新以允许跨环存储器访问。另外，关于进行调用的设备驱动器和/或跨环存储器访问的信息可以被提供给远程恶意软件分析服务器150，其可以从其它计算设备收集信息以为进行调用的设备驱动器开发或更新全局简档或“驱动器指纹”，如以下更详细讨论的。这样，可以以安全的方式且在不必针对所有设备驱动器允许或不允许所有的跨环存储器访问的情况下，在计算设备100上执行并管理传统设备驱动器，。

[0013] 计算设备100可以体现为能够执行本文描述的功能的任意类型的计算设备。例如，在一些实施例中，计算设备100可以体现为台式计算机、膝上型计算机、平板计算机、“智能”电话、移动介质设备、游戏控制台、移动互联网设备(MID)、个人数字助理、“智能”器具、或其它计算机和/或计算设备。如图1所示，计算设备100包括处理器102、存储器106、输入/输出子系统108、数据存储装置110以及通信电路112。当然，在其它实施例中，计算设备100可以包括其它或额外部件，例如通常在计算机和/或计算设备(例如，各种输入/输出设备)中找到的那些。另外，在一些实施例中，一个或多个说明性的部件可以并入另一部件或者以其他

方式形成另一部件的一部分。例如，在一些实施例中，存储器106或其部分可以并入到处理器102中。

[0014] 处理器102可以体现为能够执行本文所描述的功能的任意类型的处理器。例如，处理器可以体现为单核心处理器或具有一个或多个处理器核心104的(多个)多核心处理器、数字信号处理器、微控制器，或其它处理器或处理/控制电路。类似地，存储器106可以体现为当前已知的或将来开发的并且能够执行本文所描述的功能的任意类型的易失性或非易失性存储器或数据存储装置。在操作中，存储器106可以存储在移动计算设备100操作期间所使用的各种数据和软件，例如，操作系统、应用、程序、库和驱动器。在说明性实施例中，存储器106被分区成多个存储器区域。每个存储器区域可以被分配给不同的具有对应权限的保护域或环。例如，在说明性实施例中，存储器106包括被分配给保护环0的高权限存储器区域122(例如，内核存储器)，以及被分配给保护环3的低权限存储器区域122(例如，用户存储器)。通常，计算设备100的任何操作系统和设备驱动器将在保护环0中执行，并驻留在对应环0存储器区域120中，并且任意的用户应用和数据将在保护环3中执行，并驻留在对应环3存储器区域122中。当然，虽然说明性计算设备100被配置为具有两个保护环和对应环存储器区域，但是在其它实施例中计算设备100可以包括额外的保护环和对应环存储器区域。这样，计算设备100可以包括多层权限。

[0015] 存储器106经由I/O子系统108通信地耦合到处理器102，I/O子系统108可以体现为用于促进与处理器102、存储器106和计算设备100的其它部件的输入/输出操作的电路和/或部件。例如，I/O子系统108可以体现为或以其他方式包括存储器控制器中心、输入/输出控制中心、固件设备、通信链路(即，点到点链路、总线链路、电线、线缆、光导、印刷电路板迹线等)和/或用于促进输入/输出操作的其它部件和子系统。在一些实施例中，I/O子系统108可以形成片上系统(SoC)的一部分并且连同处理器102、存储器106和计算设备100的其它部件并入到单个集成电路芯片上。

[0016] 数据存储装置110可以体现为被配置用于短期或长期数据存储的任意类型的一个或多个设备，例如，存储器设备和电路、存储器卡、硬盘驱动装置、固态驱动装置或其它数据存储设备。在说明性实施例中，计算设备100可以在数据存储装置110内存储一个或多个设备驱动器130。每个设备驱动器130可以体现为配置为控制计算设备100的部件或电路的一个或多个软件程序或其它可执行代码。例如，设备驱动器130可以包括用于数据存储装置110的设备驱动器、用于通信电路112的设备驱动器、用于I/O子系统108的集成音频芯片或电路的设备驱动器、和/或用于计算设备100的任何其它部件、设备或电路的其它设备驱动器。如在典型的设备驱动器的情况下，每个设备驱动器130可以充当计算设备100的操作系统和对应硬件部件、设备或电路之间的软件接口。

[0017] 通信电路112可以体现为启用计算设备100和远程恶意软件分析服务器150之间通过网络160的通信的一个或多个设备和/或电路。通信电路112可以被配置为使用任意一种或多种通信技术(例如，无线或有线通信)和相关联协议(例如，以太网、蓝牙(Bluetooth®)、Wi-Fi®、WiMAX等)来实现这样的通信。

[0018] 另外，在一些实施例中，计算设备100还可以包括一个或多个外围设备114。这样的外围设备114可以包括通常在计算设备中找到的任意类型的外围设备，例如扬声器、硬件键盘、输入/输出设备、外围通信设备和/或其它外围设备。

[0019] 远程恶意软件分析服务器150可以体现为能够执行本文所描述的功能的任意类型的服务器计算设备或设备集合。远程恶意软件分析服务器150可以包括通常在服务器计算机中找到的部件和设备，包括例如处理器、I/O子系统、存储器、数据存储装置和通信电路。这样的部件可以类似于移动计算设备100的对应部件，对其的描述适用于远程恶意软件分析服务器150的对应部件，并且为了不模糊本公开不在此重复。

[0020] 远程恶意软件分析服务器150维护远程安全数据库152，其可以包括聚合和/或非聚合数据。例如，远程恶意软件分析服务器150可以聚合来自计算设备100和系统10的其它计算设备的安全数据。例如，系统10的每个计算设备100被配置为周期性、偶尔或响应性地传输安全数据到远程恶意软件分析服务器150。另外，远程安全数据库152可以包括非聚合数据，例如预加载驱动器指纹、从云或其它远程源获得的驱动器指纹等。

[0021] 安全数据可以体现为任意类型的安全数据，这些安全数据与设备驱动器130和/或设备驱动器130试图进行的跨环存储器访问相关，并且在判定设备驱动器130是否是恶意的时是有用的。例如，在一些实施例中，安全数据可以包括设备驱动器130试图执行跨环存储器访问、与设备驱动器130有关的数据(例如，试图的跨环存储器访问源自的设备驱动器130的起始地址)、和/或与试图的跨环存储器访问有关的数据(例如，设备驱动器130试图经由跨环存储器访问而访问的在另一保护环中的目的地址)。远程恶意软件分析服务器150收集这样的信息，并为每个报告的设备驱动器130建立设备驱动器简档或“驱动器指纹”154。驱动器指纹154可以体现为能用于判定设备驱动器130是否是恶意的(例如，以预期方式表现)任意类型的数据。例如，在一些实施例中，驱动器指纹154可以体现为设备驱动器130程序的位屏蔽，设备驱动器130程序通过比较位屏蔽与设备驱动器代码来判定设备驱动器130是否已经被从允许版本修改。另外地或可替代地，驱动器指纹154可以识别允许的跨环存储器访问源自的设备驱动器130的地址和/或这样的允许的跨环存储器访问的目的地址。这样，驱动器指纹154可用于分析设备驱动器130自身以及设备驱动器130的行为以判定其是否是恶意的。

[0022] 远程恶意软件分析服务器150可以周期性或偶尔以驱动器指纹154的最新拷贝来更新系统10的每个计算设备100。这样，每个计算设备100可以使用驱动器指纹154来执行设备驱动器130的本地恶意软件分析，如以下所讨论的。另外或可替代地，在一些实施例中，远程恶意软件分析服务器150可以执行这样的恶意软件分析或补充分析，并将这样的分析报告给计算设备100。

[0023] 如上所讨论的，计算设备100被配置为通过网络160与远程恶意软件分析服务器150通信。网络160可以体现为能够促进计算设备100、远程恶意软件分析服务器150和/或其它远程设备之间的通信的任意类型的网络。在说明性实施例中，网络160体现为可公开访问的全局网络，例如因特网。网络160可以包括任意数量的额外设备，例如额外远程主机、计算机、路由器和交换机，以促进计算设备100、远程恶意软件分析服务器150和/或其它设备之间的通信。

[0024] 现在参考图2，在说明性实施例中，计算设备100在操作期间建立环境200。说明性环境200包括执行一个或多个驱动器的操作系统202、安全模块204以及恶意软件分析模块206。在一些实施例中，环境200还可以包括通信模块208，如以下更详细讨论的。安全模块204、恶意软件分析模块206和/或通信模块208可以体现为软件、固件、硬件或其组合。另外，

在一些实施例中，环境200的一些或全部模块可以包括于其他模块或软件/固件结构中或形成其他模块或软件/固件结构的一部分。例如，在一些实施例中，安全模块204或其一部分可以包括于操作系统202中。

[0025] 安全模块204被配置为针对试图的跨环存储器访问而监控(多个)设备驱动器130。跨环存储器访问可以在设备驱动器130试图访问与进行调用的设备驱动器130不在同一权限域或环的存储器单元的任意时间发生。例如，如图3中说明性实施例所示，计算设备100具有安全架构，该安全架构具有两个权限保护域或环——高权限保护环0 300和较低权限保护环3 302。操作系统202和设备驱动器130在高权限保护环0 300内执行。在这样的实施例中，设备驱动器130可以访问属于保护环0 300的存储器单元，而通常不会引起异常。然而，如果设备驱动器130试图执行跨环存储器访问304以访问在保护环3 302内的存储器单元，则产生存储器异常。再次，如上所讨论的，在其它实施例中，计算设备100的安全架构可以包括额外的保护环或域。

[0026] 在一些实施例中，从较低权限到较高权限(例如，从环3 302到环0 300)的跨环存储访问是全局禁用的。在这样的实施例中，安全模块204可以主要或专门地监控如上所讨论的较高权限到较低权限存储器访问。这样，虽然说明性的计算设备100和环境200在后文中参照跨环存储器访问进行描述，但是应该理解的是这样的跨环存储器访问可以体现所有这样的存储器访问，在所述存储器访问中设备驱动器130试图访问与进行调用的设备驱动器130不在同一权限域或环内的存储器单元，或者可以体现仅目标为具有比试图的存储器访问所源自的域(即，设备驱动器130的权限域)低的权限的权限域的那些存储器访问。

[0027] 返回参考图2，安全模块204将与每个设备驱动器130相关联的存储器页表210配置为在计算设备100的引导或初始化期间(或其它适当时间)禁用跨环存储器访问。存储器页表210类似于典型的存储器页表，其提供虚拟存储器地址和设备驱动器130在计算设备100的存储器106上加载于其中的物理存储器地址之间的映射。存储器页表210包括设置，例如寄存器或标记，其可以被配置为修改存储器页表210的行为和支持功能。这样，在一些实施例中，安全模块204可以设置(即，按需要配置为逻辑高或低)存储器页表210的环3访问标记212以禁用跨环存储器访问。一旦禁用，如果相关联的设备驱动器130试图执行跨环存储器访问，则抛出异常(即，产生错误)。安全模块204被配置为截获跨环存储器访问(例如，拦截响应于试图的跨环存储器访问而抛出的异常)，并与恶意软件分析模块206接合以判定进行调用的设备驱动器130是否是恶意的。

[0028] 恶意软件分析模块206被配置为分析试图进行跨环存储器访问的设备驱动器130和/或跨环存储器访问本身，以判定设备驱动器130是否是恶意的。为此，安全模块204可以将设备驱动器130的代码或其识别数据(例如，指向存储器106中的设备驱动器130的指针)传递给恶意软件分析模块206。在一些实施例中，安全模块204还可以传递额外的相关信息，例如试图的跨环存储器访问所源自的地址以及试图的跨环存储器访问的目的地址(例如，环3地址)。恶意软件分析模块206将设备驱动器130与本地安全数据库202进行比较，以判定安全数据对于该特定设备驱动器130是否可用。如果是，则将设备驱动器130与安全数据进行比较，以判定或推断设备驱动器130是否是恶意的。例如，可以将设备驱动器130与存储于本地安全数据库220内的本地驱动器指纹222(类似于驱动器指纹154)进行比较。如上所讨论的，驱动器指纹可以体现为用于判定设备驱动器130是否为恶意的任意类型的数据。在一

些实施例中，驱动器指纹222可以体现为设备驱动器130程序的位屏蔽。在这样的实施例中，恶意软件分析模块206可以将驱动器指纹222的位屏蔽与设备驱动器130的代码进行比较，以判定设备驱动器130是否已经被修改。另外或可替代地，驱动器指纹222可以识别允许的跨环存储器访问所源自的设备驱动器130的地址和/或这样的允许的跨环存储器访问的目的地址。在这样的实施例中，恶意软件分析模块206可以将试图的跨环存储器访问的地址或进行调用的设备驱动器130的其它地址与驱动器指纹222所识别出的地址进行比较。此外，在一些实施例中，恶意软件分析模块206可以包括操作的调用堆栈以执行来判定设备驱动器130是否是恶意的和/或可以通过网络160咨询外部源，例如远程恶意软件分析服务器150。

[0029] 虽然说明性的实施例中恶意软件分析模块206被配置为分析设备驱动器130的操作以判定设备驱动器130是否是恶意的，但是恶意软件分析模块206可以另外或可替代地分析设备驱动器130的操作以判定设备驱动器130是否是“有缺陷的(buggy)”或者另外以非预期的方式操作。有缺陷的驱动器可能被其它恶意软件利用来执行未授权的访问(例如，执行历史上未被该特定设备驱动器130执行的访问)。这样，由于设备驱动器130是有缺陷的、不能信赖的或以其他方式是恶意的，所以恶意软件分析模块206判定或者以其他方式推断设备驱动器130的访问是应当被允许还是阻止。

[0030] 恶意软件分析模块206还可以分析试图的跨环存储器访问的目的环3存储器地址，以判定或推断进行调用的设备驱动器130是否是恶意的。为此，恶意软件分析模块206可以将目的地址与环3访问启发法224(或基于试图的访问的其它保护环启发法)进行比较，环3访问启发法224被维护在本地安全数据库220中。环3访问启发法224提供与针对特定环3存储器地址的访问行为相关的历史数据。如果基于历史访问数据判定对这样的存储器地址的访问为可疑的，则恶意软件分析模块206可以推断设备驱动器130是恶意的或者以恶意方式动作。应该理解的是，如果设备驱动器130不位于本地安全数据库220中，则环3访问启发法的使用可能是此时对恶意软件分析模块206仅可用的安全测量。然而，如果设备驱动器130不位于本地安全数据库220中，则恶意软件分析模块206可以将与设备驱动器130和/或试图的跨环存储器访问相关的数据传输到远程恶意软件分析服务器150，使得可以启动驱动器指纹154。如上所讨论的，远程恶意软件分析服务器150将以新的或更新后的驱动器指纹154(其作为驱动器指纹222存储于本地安全数据库220中)周期性或偶尔更新计算设备100。

[0031] 如果判定设备驱动器130不是恶意的，则安全模块204更新存储器页表210以允许试图的跨环存储器访问。然而，如果判定设备驱动器130是恶意的，则安全模块204拒绝试图的跨环存储器访问。另外，在一些实施例中，可以中断进行调用的设备驱动器130并可以产生对计算设备100的用户的警告。

[0032] 现在参考图4-6，在使用中，计算设备100可以执行用于管理由在计算设备100上执行的设备驱动器130进行的(多个)设备驱动器跨环存储器访问的方法400。方法400开始于框402，在其中初始化计算设备100。在框402期间，计算设备100可以执行各种初始化过程。例如，在框404中，计算设备100可以加载操作系统202。另外，在框406中，计算设备100的操作系统202可以加载一个或多个设备驱动器130，如上所讨论的。此外，在框408中，计算设备100可以更新本地安全数据库220。为此，恶意软件分析模块206可以经由通信模块230与远程恶意软件分析服务器150通信，以接收更新后的安全数据，例如更新后的驱动器指纹154

和/或其它安全数据。如以下更详细讨论的，这样的安全数据由计算设备100的恶意软件分析模块206使用以判定（多个）设备驱动器130是否是恶意的。虽然示出为本地安全数据库220在框408处被更新，但是应该理解的是，本地安全数据库220可以在方法400的执行期间的任意时间被更新。也就是说，计算设备100可以周期性、连续、偶尔或响应性地与远程恶意软件分析服务器150通信以接收安全数据更新，安全数据更新被存储于本地安全数据库220中。

[0033] 在框410中，计算设备100判定是否应该针对在计算设备100上加载的一个或多个设备驱动器130限制跨环存储器访问。也就是说，在一些实施例中，计算设备100可以仅针对一些设备驱动器130而监控和限制跨环存储器访问。当然，在其它实施例中，可以针对跨环存储器访问而监控加载到计算设备100上的每个设备驱动器130。

[0034] 如果针对受限的跨环存储器访问监控一个或多个设备驱动器130，则方法400前进到框412。在框412中，安全模块204将与每个被监控的设备驱动器130相关联的存储器页表210配置为禁用跨环存储器访问。如上所讨论的，存储器页表210提供虚拟存储器地址和设备驱动器130在计算设备100的存储器106中加载于其中的物理存储器地址之间的映射。另外，在说明性实施例中，存储器页表210包括控制位，其控制存储于映射的存储器单元处的软件或代码的功能（例如，允许或不允许代码做什么，代码已访问过哪些资源，等等）。安全模块204可以使用任意适当机制将存储器页表210配置为禁用通过对应设备驱动器130进行的跨环存储器访问。例如，在说明性实施例中，在框414中，安全模块204设置存储器页表210的寄存器或标记（即，取决于特定实现方式而将控制位之一配置为逻辑高或逻辑低）以禁用跨环存储器访问。因为以该方式针对（多个）设备驱动器130禁用了跨环存储器访问，所以响应于（多个）设备驱动器130的任意试图的跨环存储器访问而产生异常或错误。

[0035] 在框416中，安全模块204监控（多个）设备驱动器130的任意试图的跨环访问。如果设备驱动器130试图跨环存储器访问，则在框418中截获或以其他方式拦截试图的跨环存储器访问。为此，可以拦截或截获试图的跨环存储器访问本身，或者在一些实施例中，由试图的跨环存储器访问产生的异常或错误被拦截或截获。无论如何，在完成之前截获或拦截试图的跨环存储器访问，使得拒绝进行调用的设备驱动器130访问期望的跨环存储器。

[0036] 响应于截获/拦截试图的跨环存储器访问，安全模块204与恶意软件分析模块206接合以判定进行调用的设备驱动器130是否是恶意的。为此，安全模块204可以向恶意软件分析模块206提供设备驱动器130本身（即，设备驱动器130的代码）或标识符（例如，指向存储器中设备驱动器130的指针或其它标识符）。在框420中，恶意软件分析模块206判定进行调用的设备驱动器130是否被列在本地安全数据库220中。也就是说，恶意软件分析模块206判定进行调用的设备驱动器130的条目是否包括于本地安全数据库220中。如果进行调用的设备驱动器130未被列入到本地安全数据库220中，则试图的跨环存储器访问可能是从在计算设备100上的该特定设备驱动器130的第一次尝试，并因此，用于分析设备驱动器130的安全数据的可用性可能受到限制，如下文所讨论的。

[0037] 然而，如果进行调用的设备驱动器130被列在本地安全数据库220中，则本地安全数据库220包括能用于分析设备驱动器130的安全数据。这样，方法400前进到框422（见图5），其中恶意软件分析模块206执行对进行调用的设备驱动器130的本地恶意软件分析以判定设备驱动器130是否是恶意的。为此，恶意软件分析模块206可以将设备驱动器130与存储

于本地安全数据库220内的安全数据进行比较。例如，在框424中，恶意软件分析模块206可以将设备驱动器130与存储于本地安全数据库220中的相关联的驱动器指纹222进行比较。如上所讨论的，驱动器指纹222可以体现为能用于判定设备驱动器130是否是恶意的任意类型的数据。例如，在一些实施例中，驱动器指纹222可以体现为设备驱动器130的位屏蔽，将其与设备驱动器130的代码进行比较以判定进行调用的设备驱动器130是否已经相对于驱动器指纹222被修改。另外或可替代地，驱动器指纹222可以识别允许从其的跨环存储器访问的设备驱动器130的起始地址和/或这样的允许的跨环存储器访问的目的地址。在这样的实施例中，在框424中恶意软件分析模块206将驱动器指纹222的地址与进行调用的设备驱动器130的地址进行比较，以判定设备驱动器130是否是恶意的。

[0038] 另外，在一些实施例中，在框426中，恶意软件分析模块206可以比较与试图的跨环存储器访问的目的地址相关的启发数据。也就是说，恶意软件分析模块206可以分析先前的跨环存储器访问到试图的跨环存储器访问的目的地址以及其它相关历史访问数据，以进一步判定或推断设备驱动器130是否是恶意的。

[0039] 在框428中，恶意软件分析模块206基于框422中执行的各种分析判定设备驱动器130是否是恶意的。如果判定设备驱动器130是恶意的，则在框430中由安全模块204拒绝试图的跨环存储器访问。另外，在一些实施例中，在框432中，可以中断进行调用的设备驱动器130(例如，可以中止设备驱动器的执行)。此外，安全模块204可以在一些实施例中执行额外的安全功能，例如包括在计算设备100上产生警告以通知用户安全扰乱，发送关于安全扰乱和/或进行调用的设备驱动器130的信息到远程恶意软件分析服务器150，和/或其它安全功能。在框430中拒绝了试图的跨环存储器访问之后，方法400循环回到框416(见图4)，其中安全模块204继续针对跨环存储器访问进行监控。

[0040] 返回参考框428，如果判定跨环存储器访问不是恶意的，则方法400前进的到框434，在其中安全模块204更新存储器页表210以允许设备驱动器130的试图的跨环存储器访问。为此，例如，在框436中，安全模块204可以重置/设置存储器页表210的标记或寄存器，以允许试图的跨环存储器访问。在框434中启用试图的跨环存储器访问之后，方法400循环回到框416(见图4)，其中安全模块204继续针对跨环存储器访问进行监控。

[0041] 返回参考框420，如果进行调用的设备驱动器130未被列在本地安全数据库220中，则方法400前进到框438(见图6)，其中恶意软件分析模块206试图执行对进行调用的设备驱动器130的本地恶意软件分析。然而，因为对于进行调用的设备驱动器130没有可用的驱动器指纹222，所以在框440中，恶意软件分析模块206试图仅使用与试图的跨环存储器访问的目的地址相关的启发数据(如果可用)来判定或推断设备驱动器130是否是恶意的。在一些实施例中，如果没有可用的启发数据，则恶意软件分析模块206可以假设设备驱动器130不是恶意的。可替代地，在其它实施例中，如果没有启发数据可用于执行足够的分析，则恶意软件分析模块206可以假设设备驱动器130是恶意的。

[0042] 无论如何，在框442中，恶意软件分析模块206更新本地安全数据库220。也就是说，在一些实施例中，恶意软件分析模块206可以为未知的进行调用的设备驱动器130产生新的驱动器指纹222。驱动器指纹222可以包括与进行调用的设备驱动器130相关的安全数据和/或与试图的跨环存储器访问相关的目的/起始存储器地址。另外或可替代地，恶意软件分析模块206可以将这样的安全数据传输到远程恶意软件分析服务器150，以允许远程恶意软件

分析服务器150产生或更新用于进行调用的设备驱动器130的驱动器指纹154。随着时间经过，以额外的安全数据更新驱动器指纹154、222，直到驱动器指纹154、222实质上足够促进使用这样的驱动器指纹154、222对设备驱动器130的分析。如上所讨论的，恶意软件分析模块206可以以来自远程恶意软件分析服务器150的安全数据（例如，新的或更新后的驱动器指纹222）来周期性或偶尔更新本地安全数据库220。

[0043] 随后，在框446中，恶意软件分析模块206基于在框438中执行的分析（如果有的话）判定设备驱动器130是否是恶意的。如果判定（或假设）设备驱动器130是恶意的，则在框448中由安全模块204拒绝试图的跨环存储器访问。另外，如上所讨论的，在一些实施例中，在框450中可以中断进行调用的设备驱动器130。此外，在一些实施例中，安全模块204可以执行额外的或其它的安全功能。在框448中拒绝试图的跨环存储器访问之后，方法400循环回到框416（见图4），其中安全模块204继续针对跨环存储器访问进行监控。

[0044] 返回参考框446，如果判定（或假设）跨环存储器访问不是恶意的，则方法400前进到框452，其中安全模块204更新存储器页表210以允许设备驱动器130的试图的跨环存储器访问。为此，在框554中，安全模块204可以重置/设置存储器页表210的标记或寄存器，以允许试图的跨环存储器访问，如上所讨论的。在框452中启用试图的跨环存储器访问之后，方法400循环回到框416（见图4），其中安全模块204继续针对跨环存储器访问进行监控。

[0045] 例子

[0046] 下面提供了本文公开的技术的说明性例子。该技术的实施例可以包括任意一个或多个以下描述的例子或其组合。

[0047] 例子1包括一种用于管理在计算设备上的设备驱动器的跨环存储器访问的计算设备，所述计算设备包括：安全模块，用于（i）将与所述设备驱动器相关联的存储器页表配置为禁用所述设备驱动器的跨环存储器访问，以及（ii）在配置相关联的存储器页表之后截获所述设备驱动器的试图的跨环存储器访问；以及恶意软件分析模块，用于响应于截获所述试图的跨环存储器访问而分析所述设备驱动器，以判定所述设备驱动器是否是恶意的，其中，所述安全模块还用于响应于所述恶意软件分析模块判定所述设备驱动器是恶意的而拒绝所述试图的跨环存储器访问。

[0048] 例子2包括例子1的主题，并且其中，所述安全模块还用于响应于所述恶意软件分析模块判定所述设备驱动器不是恶意的，而更新与所述设备驱动器相关联的存储器页表，以允许所述试图的跨环存储器访问。

[0049] 例子3包括例子1和2中任一个的主题，并且其中，所述安全模块用于设置所述存储器页表中的标记，以禁用所述设备驱动器的跨环存储器访问。

[0050] 例子4包括例子1-3中任一个的主题，并且还包括操作系统，用于在所述计算设备的较高权限环中执行所述设备驱动器，并且其中，所述安全模块用于设置所述存储器页表中的标记，以禁用所述计算设备的从较高权限环到较低权限环的存储器访问。

[0051] 例子5包括例子1-4中任一个的主题，并且其中，所述安全模块用于截获源自所述计算设备上建立的第一保护环到在所述计算设备上建立的不同于所述第一保护环的第二保护环的存储器访问。

[0052] 例子6包括例子1-5中任一个的主题，并且其中，所述安全模块用于截获所述计算设备上执行的每个设备驱动器试图进行的所有跨环存储器访问。

[0053] 例子7包括例子1-6中任一个的主题，并且其中，所述恶意软件分析模块用于将所述设备驱动器与存储于本地安全数据库中的安全数据进行比较，以判定所述设备驱动器是否是恶意的。

[0054] 例子8包括例子1-7中任一个的主题，并且其中，所述恶意软件分析模块用于匹配所述设备驱动器与存储于本地安全数据库中的参考设备驱动器；以及将所述参考设备驱动器的驱动器指纹与所述设备驱动器进行比较。

[0055] 例子9包括例子1-8中任一个的主题，并且其中，所述恶意软件分析模块用于将所述驱动器指纹的地址与所述试图的跨环存储器访问所源自的所述设备驱动器的地址进行比较。

[0056] 例子10包括例子1-9中任一个的主题，并且其中，所述恶意软件分析模块用于将位屏蔽与和所述设备驱动器相关联的存储器页表进行比较。

[0057] 例子11包括例子1-10中任一个的主题，并且其中，所述恶意软件分析模块用于将与所述参考设备驱动器相关联的多个地址和与所述设备驱动器相关联的地址进行比较。

[0058] 例子12包括例子1-11中任一个的主题，并且其中，所述恶意软件分析模块还用于从远程恶意软件分析服务器接收用于所述设备驱动器的更新后的驱动器指纹，并将更新后的驱动器指纹存储于所述本地安全数据库中。

[0059] 例子13包括例子1-12中任一个的主题，并且其中，所述恶意软件分析模块用于判定所述设备驱动器是否与存储于本地安全数据库中的参考设备驱动器匹配；以及响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考驱动器不匹配，而产生用于所述设备驱动器的驱动器指纹。

[0060] 例子14包括例子1-13中任一个的主题，并且其中，所述恶意软件分析模块用于产生识别所述设备驱动器的跨环存储器访问源自的地址的驱动器指纹。

[0061] 例子15包括例子1-14中任一个的主题，并且其中，所述恶意软件分析模块还用于将产生的驱动器指纹发送给远程恶意软件分析服务器。

[0062] 例子16包括例子1-15中任一个的主题，并且其中，所述恶意软件分析模块用于判定所述设备驱动器是否与存储于所述本地安全数据库中的参考设备驱动器匹配；以及响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考设备驱动器不匹配，而更新与所述设备驱动器相关联的存储器页表以允许所述试图的跨环存储器访问。

[0063] 例子17包括例子1-16中任一个的主题，并且其中，所述恶意软件分析模块用于重置所述存储器页表中的标记以启用所述设备驱动器的跨环存储器访问。

[0064] 例子18包括例子1-17中任一个的主题，并且其中，所述恶意软件分析模块用于将所述试图的跨环存储器访问的目的地址与存储于本地安全数据库中的安全数据进行比较，以判定所述设备驱动器是否是恶意的。

[0065] 例子19包括例子1-18中任一个的主题，并且其中，所述恶意软件分析模块用于将所述试图的跨环存储器访问的目的地址与先前跨环存储器访问到所述目的地址的启发数据进行比较。

[0066] 例子20包括例子1-19中任一个的主题，并且其中，所述恶意软件分析模块用于将所述试图的跨环存储器访问的保护环3目的地址与存储于所述本地安全数据库中的保护环3地址进行比较。

[0067] 例子21包括例子1-20中任一个的主题，并且其中，所述安全模块用于响应于所述恶意软件分析模块判定所述设备驱动器是恶意的，而中断所述设备驱动器。

[0068] 例子22包括例子1-21中任一个的主题，并且其中，所述安全模块用于重置所述存储器页表中的标记以启用所述设备驱动器的跨环存储器访问。

[0069] 例子23包括例子1-22中任一个的主题，并且其中，所述安全模块用于响应于判定所述设备驱动器是恶意的，而所述在计算设备上产生警告。

[0070] 例子24包括例子1-23中任一个的主题，并且其中，所述恶意软件分析模块还用于从远程恶意软件分析服务器接收用于所述设备驱动器的更新后的驱动器指纹，并将更新后的驱动器指纹存储于本地安全数据库中。

[0071] 例子25包括一种用于管理在计算设备上的设备驱动器的跨环存储器访问的方法，所述方法包括：在所述计算设备上，将与所述设备驱动器相关联的存储器页表配置为禁用所述设备驱动器的跨环存储器访问；在配置相关联的存储器页表之后，截获所述设备驱动器的试图的跨环存储器访问；响应于截获所述试图的跨环存储器访问而分析所述设备驱动器，以判定所述设备驱动器是否是恶意的；以及响应于判定所述设备驱动器是恶意的而拒绝所述试图的跨环存储器访问。

[0072] 例子26包括例子25的主题，并且还包括响应于判定所述设备驱动器不是恶意的，而更新与所述设备驱动器相关联的存储器页表，以允许所述试图的跨环存储器访问。

[0073] 例子27包括例子25和26中任一个的主题，并且其中，配置与所述设备驱动器相关联的存储器页表包括：设置所述存储器页表中的标记，以禁用所述设备驱动器的跨环存储器访问。

[0074] 例子28包括例子25-27中任一个的主题，并且还包括在所述计算设备的较高权限环中执行所述设备驱动器，并且其中，设置所述存储器页表中的标记包括设置所述存储器页表中的标记以禁用所述计算设备的从较高权限环到较低权限环的存储器访问。

[0075] 例子29包括例子25-28中任一个的主题，并且其中，截获试图的跨环存储器访问包括：截获源自所述计算设备上建立的第一保护环到在所述计算设备上建立的不同于所述第一保护环的第二保护环的存储器访问。

[0076] 例子30包括例子25-29中任一个的主题，并且其中，截获试图的跨环存储器访问包括：截获所述计算设备上执行的每个设备驱动器所试图进行的所有跨环存储器访问。

[0077] 例子31包括例子25-30中任一个的主题，并且其中，分析所述设备驱动器包括：将所述设备驱动器与存储于本地安全数据库中的安全数据进行比较，以判定所述设备驱动器是否是恶意的。

[0078] 例子32包括例子25-31中任一个的主题，并且其中，分析所述设备驱动器包括：匹配所述设备驱动器与存储于本地安全数据库中的参考设备驱动器；以及将所述参考设备驱动器的驱动器指纹与所述设备驱动器进行比较。

[0079] 例子33包括例子25-32中任一个的主题，并且其中，比较所述驱动器指纹包括：将所述驱动器指纹的地址与所述试图的跨环存储器访问所源自的所述设备驱动器的地址进行比较。

[0080] 例子34包括例子25-33中任一个的主题，并且其中，比较所述驱动器指纹包括：将位屏蔽与和所述设备驱动器相关联的存储器页表进行比较。

[0081] 例子35包括例子25-34中任一个的主题，并且其中，比较所述驱动器指纹包括：将与所述参考设备驱动器相关联的多个地址和与所述设备驱动器相关联的地址进行比较。

[0082] 例子36包括例子25-35中任一个的主题，并且还包括从远程恶意软件分析服务器接收用于所述设备驱动器的更新后的驱动器指纹，并将更新后的驱动器指纹存储于所述本地安全数据库中。

[0083] 例子37包括例子25-36中任一个的主题，并且其中，分析所述设备驱动器包括：判定所述设备驱动器是否与存储于本地安全数据库中的参考设备驱动器匹配；以及响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考驱动器不匹配，而产生用于所述设备驱动器的驱动器指纹。

[0084] 例子38包括例子25-37中任一个的主题，并且其中，产生驱动器指纹包括：产生识别所述设备驱动器的跨环存储器访问源自的地址的驱动器指纹。

[0085] 例子39包括例子25-38中任一个的主题，并且还包括将产生的驱动器指纹发送给远程恶意软件分析服务器。

[0086] 例子40包括例子25-39中任一个的主题，并且其中，分析所述设备驱动器包括：判定所述设备驱动器是否与存储于所述本地安全数据库中的参考设备驱动器匹配；以及响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考设备驱动器不匹配，而更新与所述设备驱动器相关联的存储器页表以允许所述试图的跨环存储器访问。

[0087] 例子41包括例子25-40中任一个的主题，并且其中，更新与所述设备驱动器相关联的存储器页表包括：重置所述存储器页表中的标记以启用所述设备驱动器的跨环存储器访问。

[0088] 例子42包括例子25-41中任一个的主题，并且其中，分析所述试图的跨环存储器访问包括：将所述试图的跨环存储器访问的目的地址与存储于本地安全数据库中的安全数据进行比较，以判定所述设备驱动器是否是恶意的。

[0089] 例子43包括例子25-42中任一个的主题，并且其中，比较所述试图的跨环存储器访问的目的地址包括：将所述试图的跨环存储器访问的目的地址与先前跨环存储器访问到所述目的地址的启发数据进行比较。

[0090] 例子44包括例子25-43中任一个的主题，并且其中，比较所述试图的跨环存储器访问的目的地址包括：将试图的跨环存储器访问的保护环3目的地址与存储于所述本地安全数据库中的保护环3地址进行比较。

[0091] 例子45包括例子25-44中任一个的主题，并且其中，拒绝所述试图的跨环存储器访问包括中断所述设备驱动器。

[0092] 例子46包括例子25-45中任一个的主题，并且其中，更新与所述设备驱动器相关联的存储器页表包括：重置所述存储器页表中的标记以启用所述设备驱动器的跨环存储器访问。

[0093] 例子47包括例子25-46中任一个的主题，并且还包括：响应于判定所述设备驱动器是恶意的，而在所述计算设备上产生警告。

[0094] 例子48包括例子25-47中任一个的主题，并且还包括：从远程恶意软件分析服务器接收用于所述设备驱动器的更新后的驱动器指纹，并将更新后的驱动器指纹存储于本地安全数据库中。

[0095] 例子49包括一种计算设备，其包括处理器；以及具有存储于其中多个指令的存储器，当被处理器执行时，所述指令使得所述计算设备执行如例子25-48中任一个所述的方法。

[0096] 例子50包括一种或多种包括存储于其上的多个指令的机器可读存储介质，响应于被执行，所述指令导致计算设备执行如例子25-48中任一个所述的方法。

[0097] 例子51包括一种用于管理跨环存储器访问的计算设备，所述计算设备包括：用于将与设备驱动器相关联的存储器页表配置为禁用所述设备驱动器的跨环存储器访问的装置；用于在配置相关联的存储器页表之后截获所述设备驱动器的试图的跨环存储器访问的装置；用于响应于截获所述试图的跨环存储器访问而分析所述设备驱动器以判定所述设备驱动器是否是恶意的装置；以及用于响应于判定所述设备驱动器是恶意的而拒绝所述试图的跨环存储器访问的装置。

[0098] 例子52包括例子51的主题，并且还包括用于响应于判定所述设备驱动器不是恶意的，而更新与所述设备驱动器相关联的存储器页表，以允许所述试图的跨环存储器访问的装置。

[0099] 例子53包括例子51和52中任一个的主题，并且其中，用于配置与设备驱动器相关联的存储器页表的装置包括：用于设置所述存储器页表中的标记，以禁用所述设备驱动器的跨环存储器访问的装置。

[0100] 例子54包括例子51-53中任一个的主题，并且还包括用于在所述计算设备的较高权限环中执行所述设备驱动器的装置，并且其中，用于设置所述存储器页表中的标记的装置包括：用于设置所述存储器页表中的标记以禁用所述计算设备的从较高权限环到较低权限环的存储器访问的装置。

[0101] 例子55包括例子51-54中任一个的主题，并且其中，用于截获试图的跨环存储器访问的装置包括：用于截获源自所述计算设备上建立的第一保护环到在所述计算设备上建立的不同于所述第一保护环的第二保护环的存储器访问的装置。

[0102] 例子56包括例子51-55中任一个的主题，并且其中，用于截获试图的跨环存储器访问的装置包括：用于截获所述计算设备上执行的每个设备驱动器所试图进行的所有跨环存储器访问的装置。

[0103] 例子57包括例子51-56中任一个的主题，并且其中，用于分析所述设备驱动器的装置包括：用于将所述设备驱动器与存储于本地安全数据库中的安全数据进行比较，以判定所述设备驱动器是否是恶意的装置。

[0104] 例子58包括例子51-57中任一个的主题，并且其中，用于分析所述设备驱动器的装置包括：用于匹配所述设备驱动器与存储于本地安全数据库中的参考设备驱动器的装置；以及用于将所述参考设备驱动器的驱动器指纹与所述设备驱动器进行比较的装置。

[0105] 例子59包括例子51-58中任一个的主题，并且其中，用于比较所述驱动器指纹的装置包括：用于将所述驱动器指纹的地址与所述试图的跨环存储器访问所源自的所述设备驱动器的地址进行比较的装置。

[0106] 例子60包括例子51-59中任一个的主题，并且其中，用于比较所述驱动器指纹的装置包括：用于将位屏蔽与和所述设备驱动器相关联的存储器页表进行比较的装置。

[0107] 例子61包括例子51-60中任一个的主题，并且其中，用于比较所述驱动器指纹的装

置包括：用于将与所述参考设备驱动器相关联的多个地址和与所述设备驱动器相关联的地址进行比较的装置。

[0108] 例子62包括例子51-61中任一个的主题，并且还包括用于从远程恶意软件分析服务器接收用于所述设备驱动器的更新后的驱动器指纹的装置，以及用于将更新后的驱动器指纹存储于所述本地安全数据库中的装置。

[0109] 例子63包括例子51-62中任一个的主题，并且其中，用于分析所述设备驱动器的装置包括：用于判定所述设备驱动器是否与存储于本地安全数据库中的参考设备驱动器匹配的装置；以及用于响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考驱动器不匹配，而产生用于所述设备驱动器的驱动器指纹的装置。

[0110] 例子64包括例子51-63中任一个的主题，并且其中，用于产生驱动器指纹的装置包括：用于产生识别所述设备驱动器的跨环存储器访问源自的地址的驱动器指纹的装置。

[0111] 例子65包括例子51-64中任一个的主题，并且还包括用于将产生的驱动器指纹发送给远程恶意软件分析服务器的装置。

[0112] 例子66包括例子51-65中任一个的主题，并且其中，用于分析所述设备驱动器的装置包括：用于判定所述设备驱动器是否与存储于所述本地安全数据库中的参考设备驱动器匹配的装置；以及用于响应于所述设备驱动器与存储于所述本地安全数据库中的任意参考设备驱动器不匹配，而更新与所述设备驱动器相关联的存储器页表以允许所述试图的跨环存储器访问的装置。

[0113] 例子67包括例子51-66中任一个的主题，并且其中，用于更新与设备驱动器相关联的存储器页表的装置包括：用于重置所述存储器页表中的标记以启用所述设备驱动器的跨环存储器访问的装置。

[0114] 例子68包括例子51-67中任一个的主题，并且其中，用于分析所述试图的跨环存储器访问的装置包括：用于将所述试图的跨环存储器访问的目的地址与存储于本地安全数据库中的安全数据进行比较，以判定所述设备驱动器是否是恶意的装置。

[0115] 例子69包括例子51-68中任一个的主题，并且其中，用于比较所述试图的跨环存储器访问的目的地址的装置包括：用于将所述试图的跨环存储器访问的目的地址与先前跨环存储器访问到所述目的地址的启发数据进行比较的装置。

[0116] 例子70包括例子51-69中任一个的主题，并且其中，用于比较所述试图的跨环存储器访问的目的地址的装置包括：用于将所述试图的跨环存储器访问的保护环3目的地址与存储于所述本地安全数据库中的保护环3地址进行比较的装置。

[0117] 例子71包括例子51-70中任一个的主题，并且其中，用于拒绝所述试图的跨环存储器访问的装置包括：用于中断所述设备驱动器的装置。

[0118] 例子72包括例子51-71中任一个的主题，并且其中，用于更新与所述设备驱动器相关联的存储器页表的装置包括：用于重置所述存储器页表中的标记以启用所述设备驱动器的跨环存储器访问的装置。

[0119] 例子73包括例子51-72中任一个的主题，并且还包括：用于响应于判定所述设备驱动器是恶意的，而在所述计算设备上产生警告的装置。

[0120] 例子74包括例子51-73中任一个的主题，并且还包括：用于从远程恶意软件分析服务器接收用于所述设备驱动器的更新后的驱动器指纹的装置，以及用于将更新后的驱动器

指纹存储于本地安全数据库中的装置。

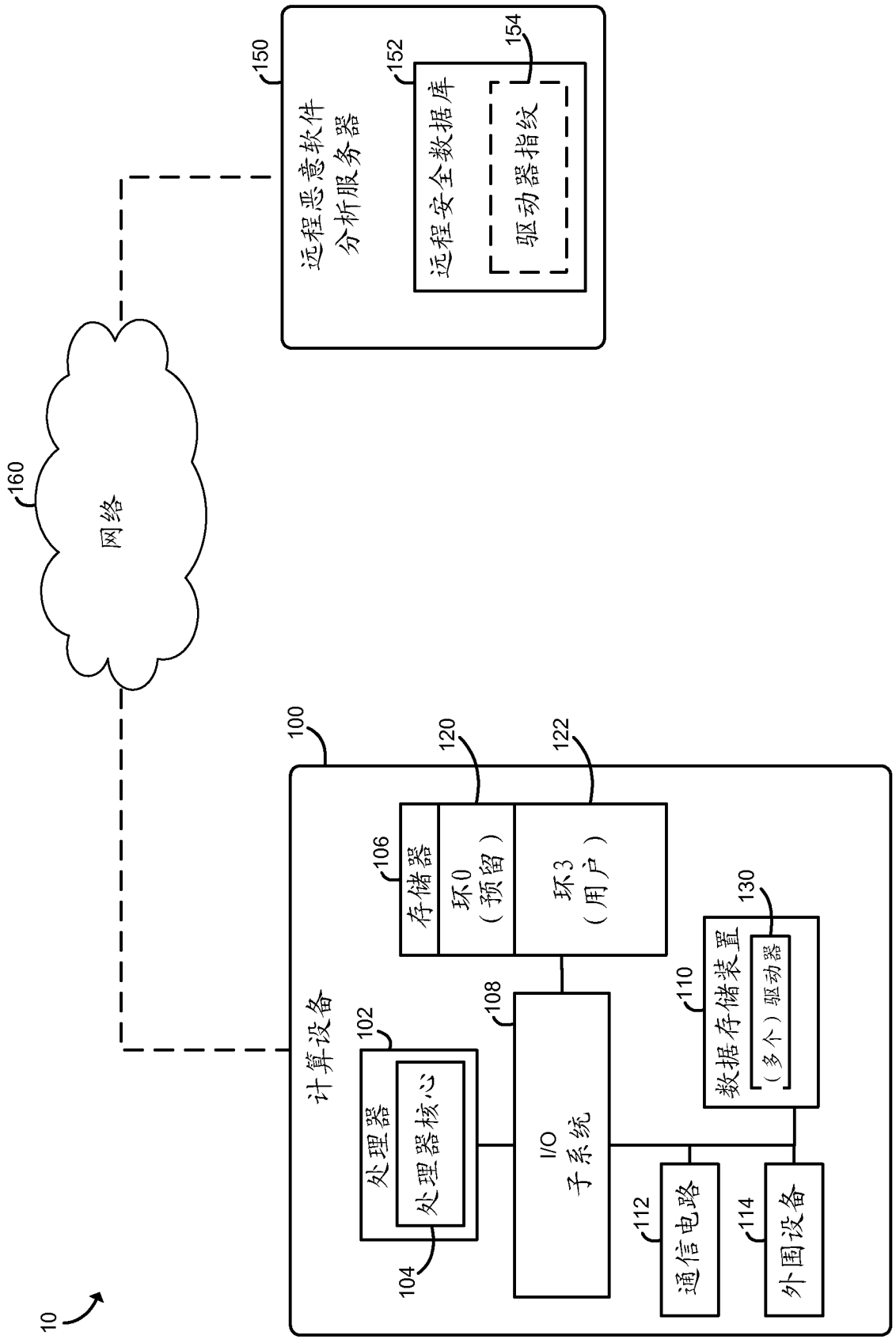

10
计算设备
100
处理器
处理器核心
102
104
存储器
106
环0
（预留）
环3
（用户）
120
122
I/O
子系统
108
通信电路
112
外围设备
114
数据存储装置
（多个）驱动器
110
130
网络
160
远程恶意软件
分析服务器
150
远程安全数据库
驱动器指纹
152
154

图 1

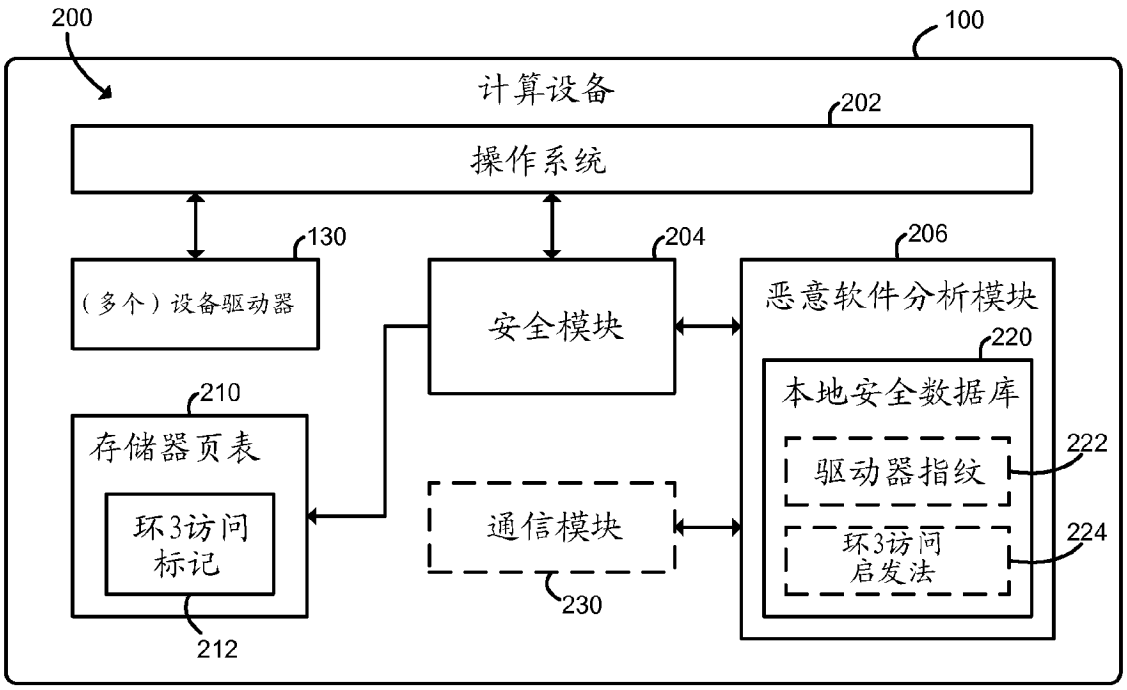

200
100
计算设备
202
操作系统
130
(多个)设备驱动器
204
安全模块
206
恶意软件分析模块
220
本地安全数据库
222
驱动器指纹
224
环3访问
启发法
210
存储器页表
环3访问
标记
212
通信模块
230

图 2

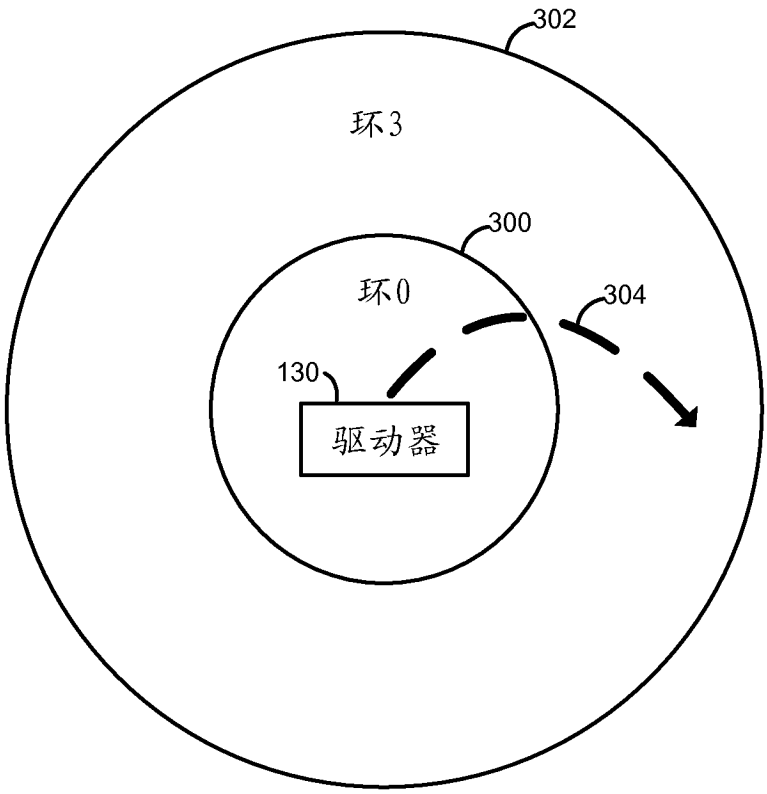

302
环3
300
环0
304
130
驱动器

图 3

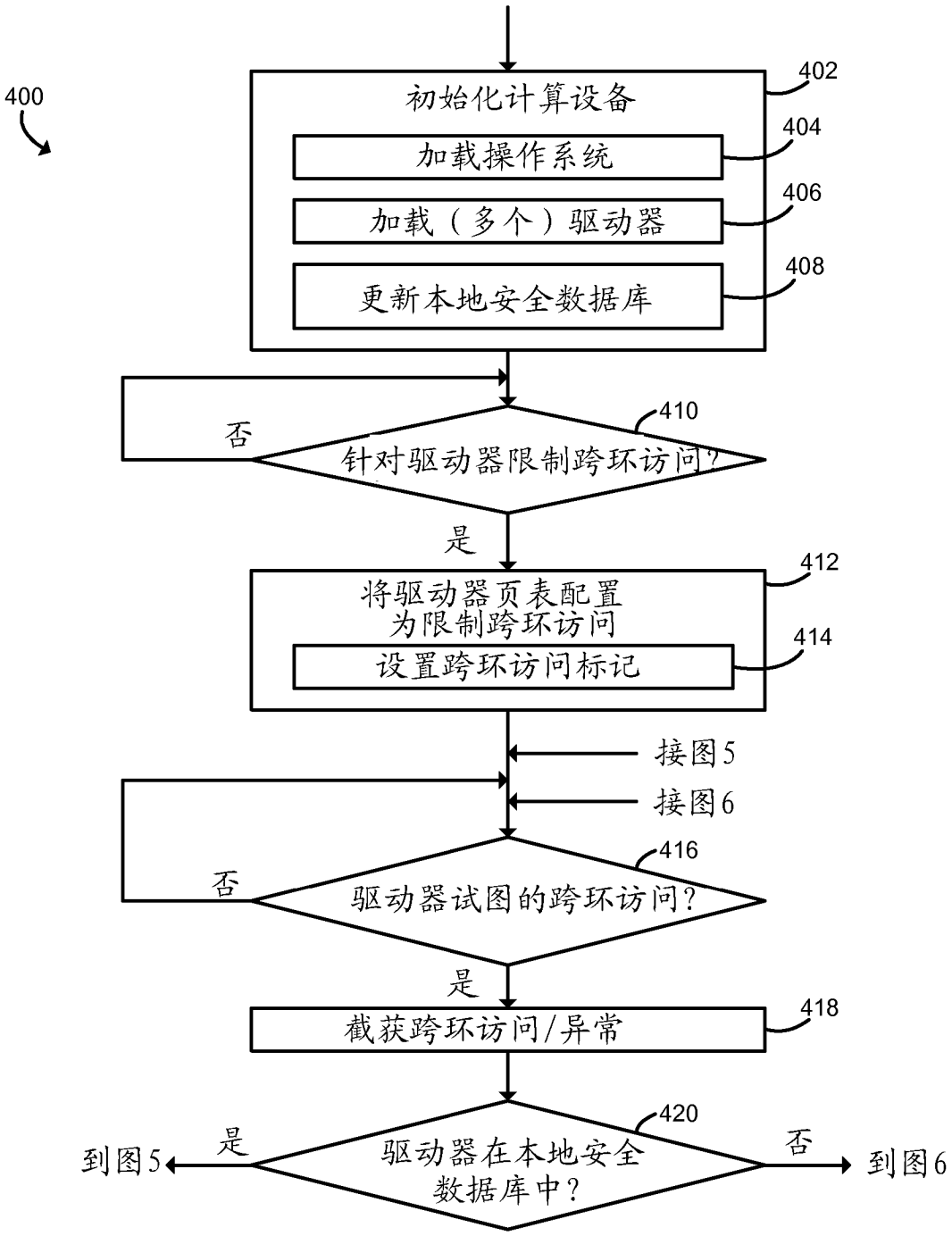

400
初始化计算设备
402
加载操作系统
404
加载（多个）驱动器
406
更新本地安全数据库
408
否
针对驱动器限制跨环访问？
410
是
将驱动器页表配置
为限制跨环访问
412
设置跨环访问标记
414
接图5
接图6
否
驱动器试图的跨环访问？
416
是
截获跨环访问/异常
418
是
驱动器在本地安全
数据库中？
420
否
到图5
到图6

图 4

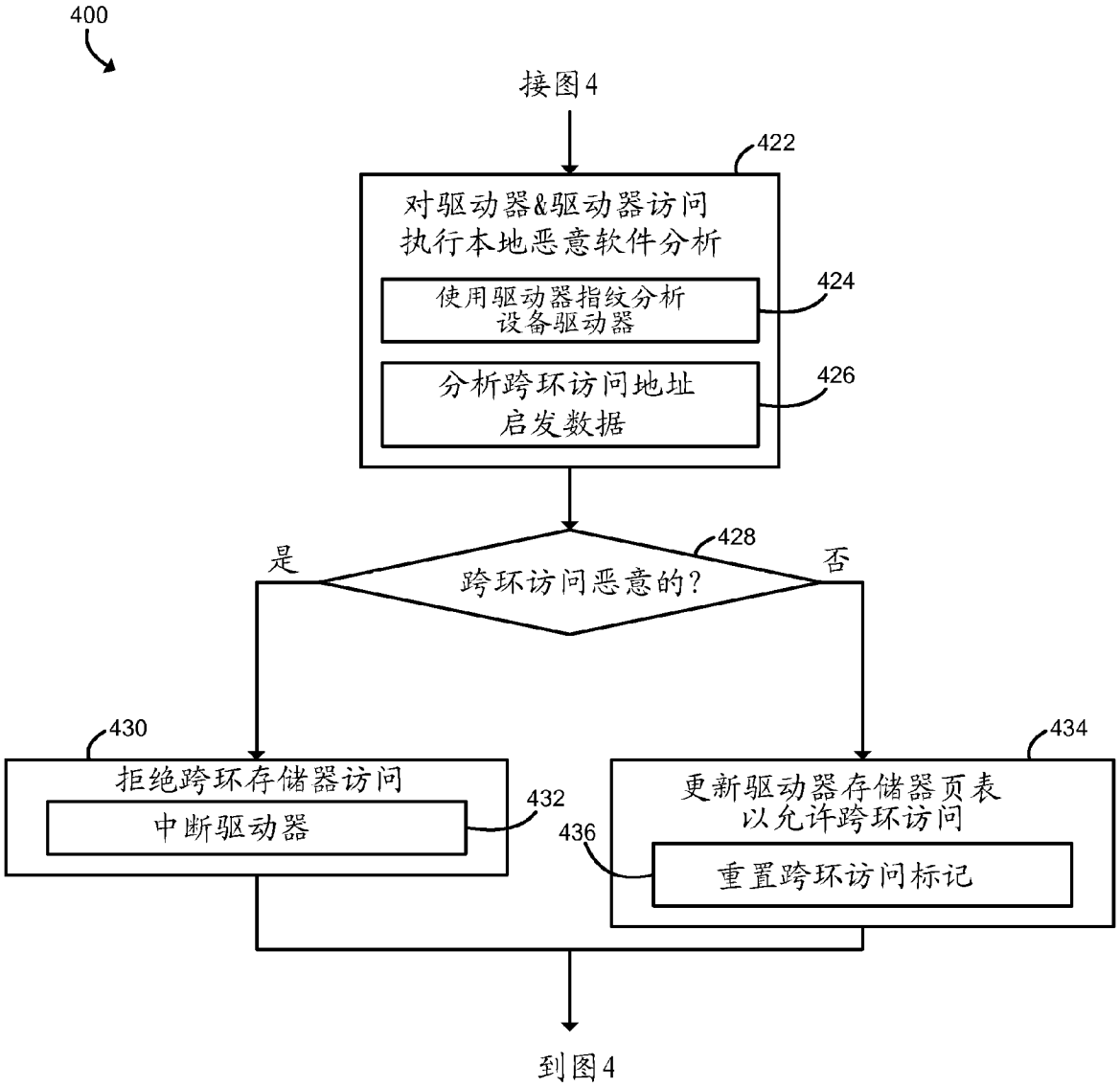

400
接图4
422
对驱动器&驱动器访问
执行本地恶意软件分析
424
使用驱动器指纹分析
设备驱动器
426
分析跨环访问地址
启发数据
428
是
跨环访问恶意的?
否
430
拒绝跨环存储器访问
432
中断驱动器
434
更新驱动器存储器页表
以允许跨环访问
436
重置跨环访问标记
到图4

图 5

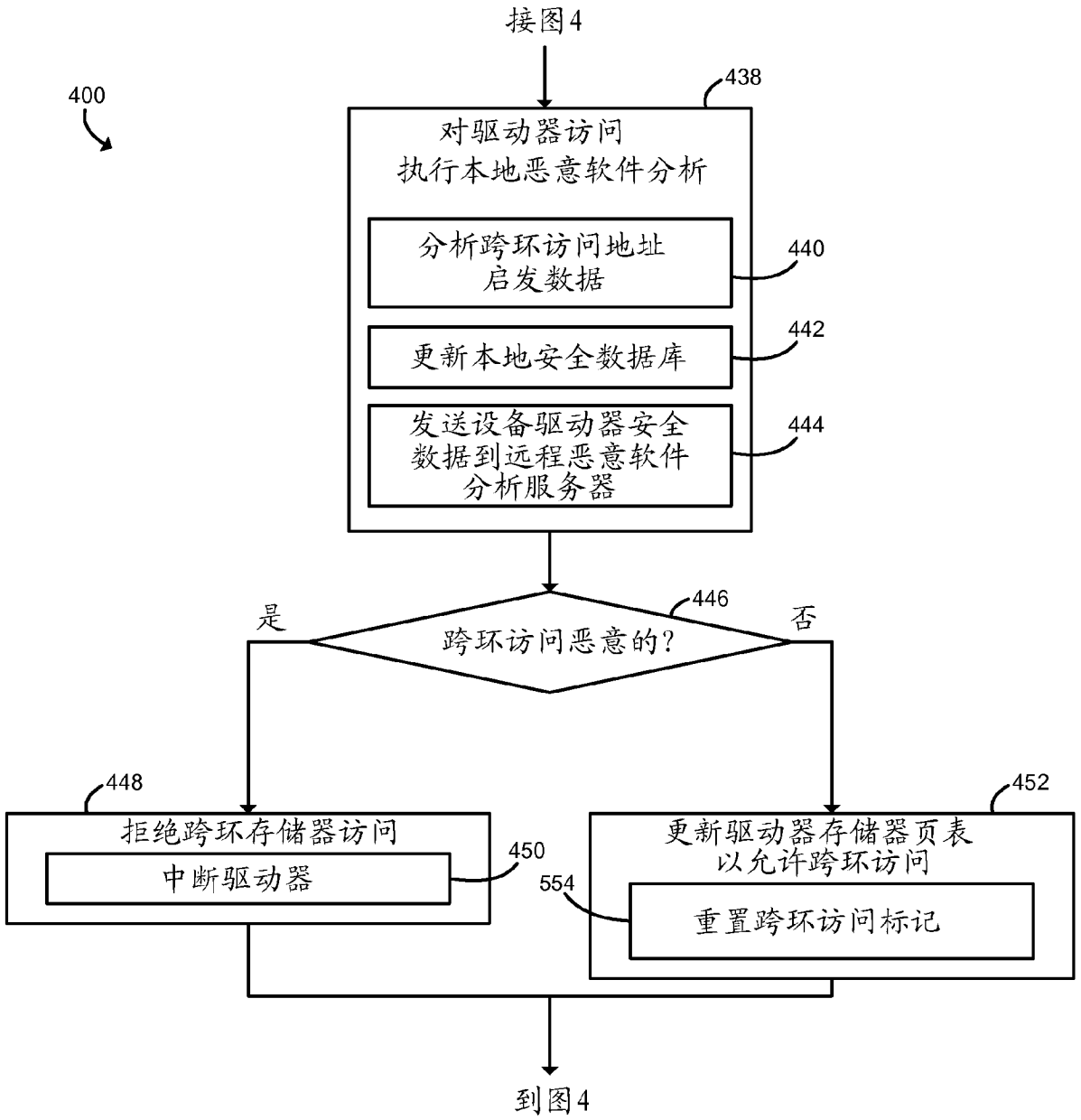

接图4
400
438
对驱动器访问
执行本地恶意软件分析
分析跨环访问地址
启发数据
440
更新本地安全数据库
442
发送设备驱动器安全
数据到远程恶意软件
分析服务器
444
446
是
跨环访问恶意的?
否
448
拒绝跨环存储器访问
中断驱动器
450
452
更新驱动器存储器页表
以允许跨环访问
554
重置跨环访问标记
到图4

图 6